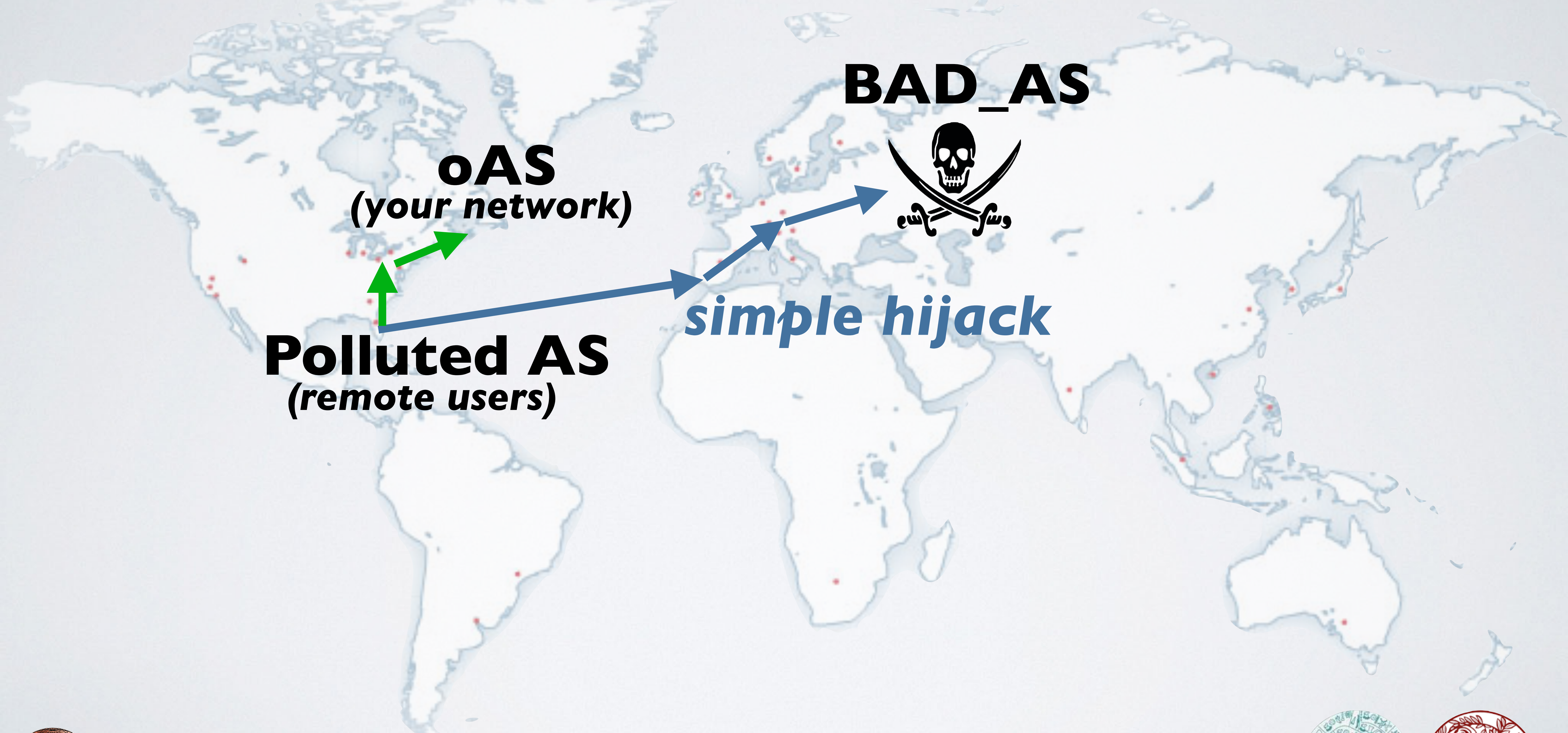
Detecting Internet Traffic Interception based on Route Hijacking

Alberto Dainotti
alberto@caida.org
Center for Applied Internet Data Analysis
University of California, San Diego

Joint work with:
Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas Dimitropoulos, Jae Hyun Park, Danilo Cicalese, Alistair King

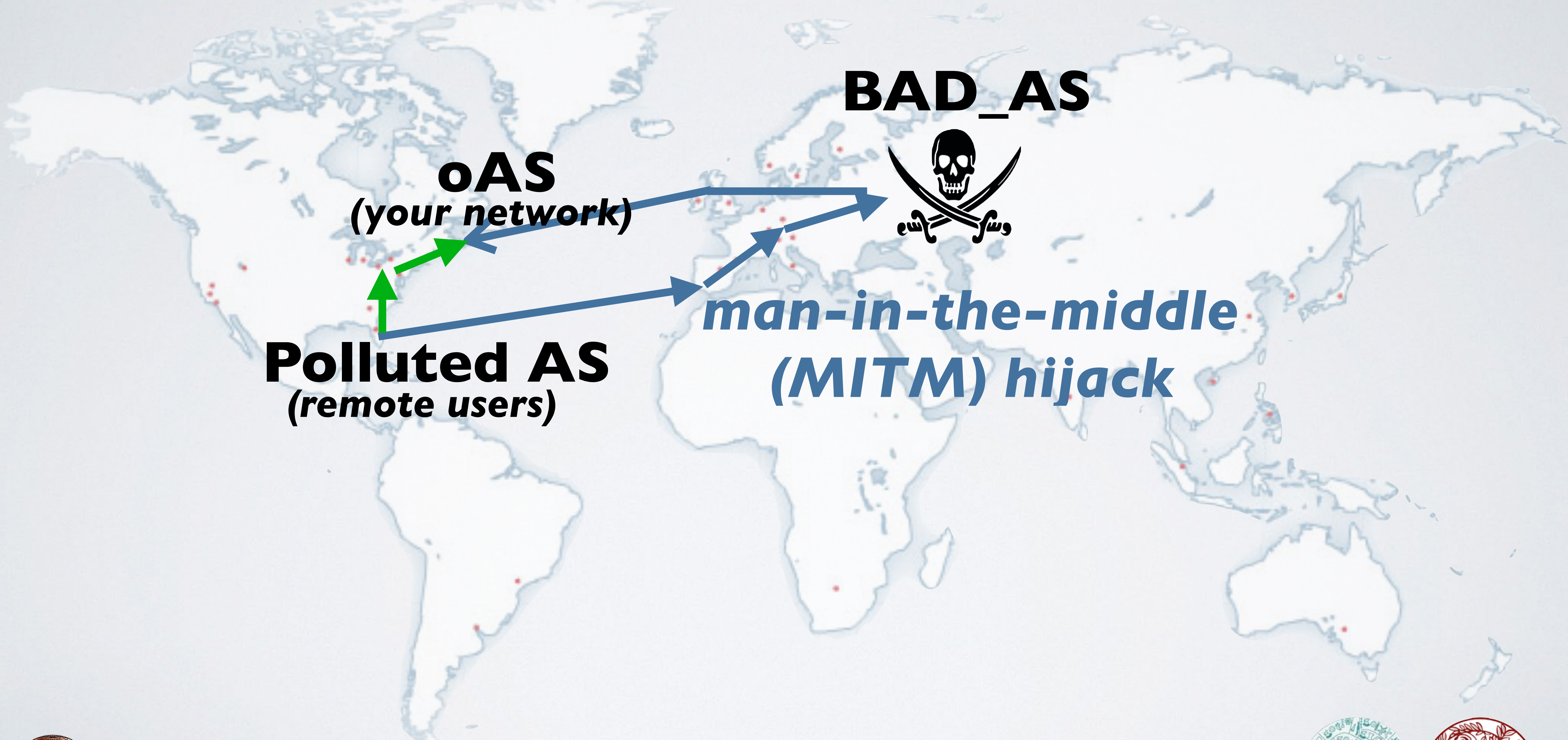
INTERNET ROUTE HIJACKING

a threat to your organization and to critical infrastructure



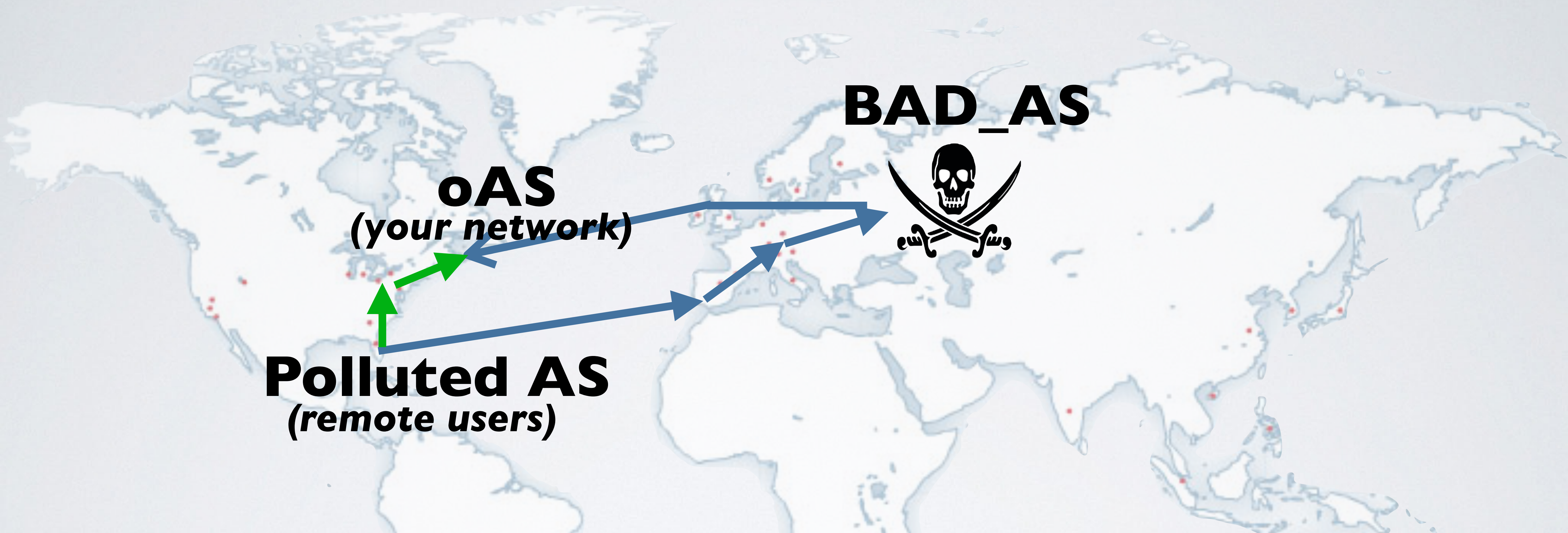
INTERNET ROUTE HIJACKING

a threat to your organization and to critical infrastructure

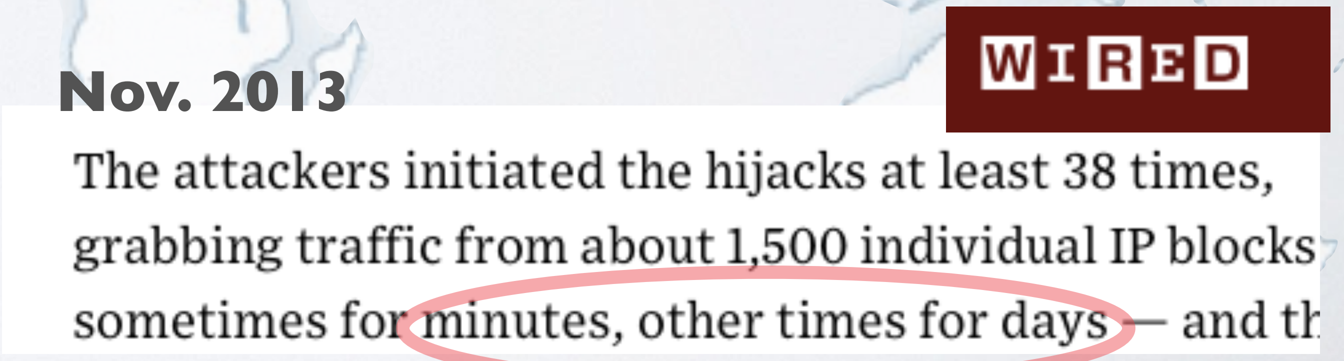


INTERNET ROUTE HIJACKING

many **MITM** *events documented*



Nov. 2013

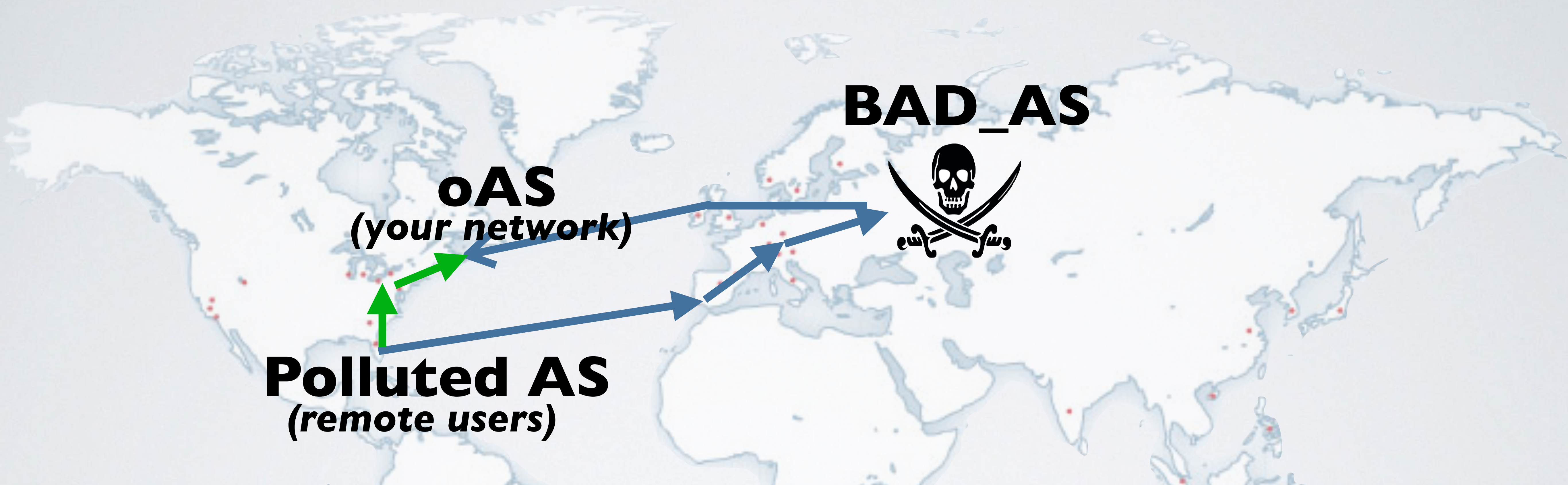

WIRED

The attackers initiated the hijacks at least 38 times, grabbing traffic from about 1,500 individual IP blocks, sometimes for minutes, other times for days — and th

http://research.dyn.com/2013/11/mitm-internet-hijacking/

INTERNET ROUTE HIJACKING

many **MITM** *events documented*



In few minutes, a single attack can manipulate millions of flows

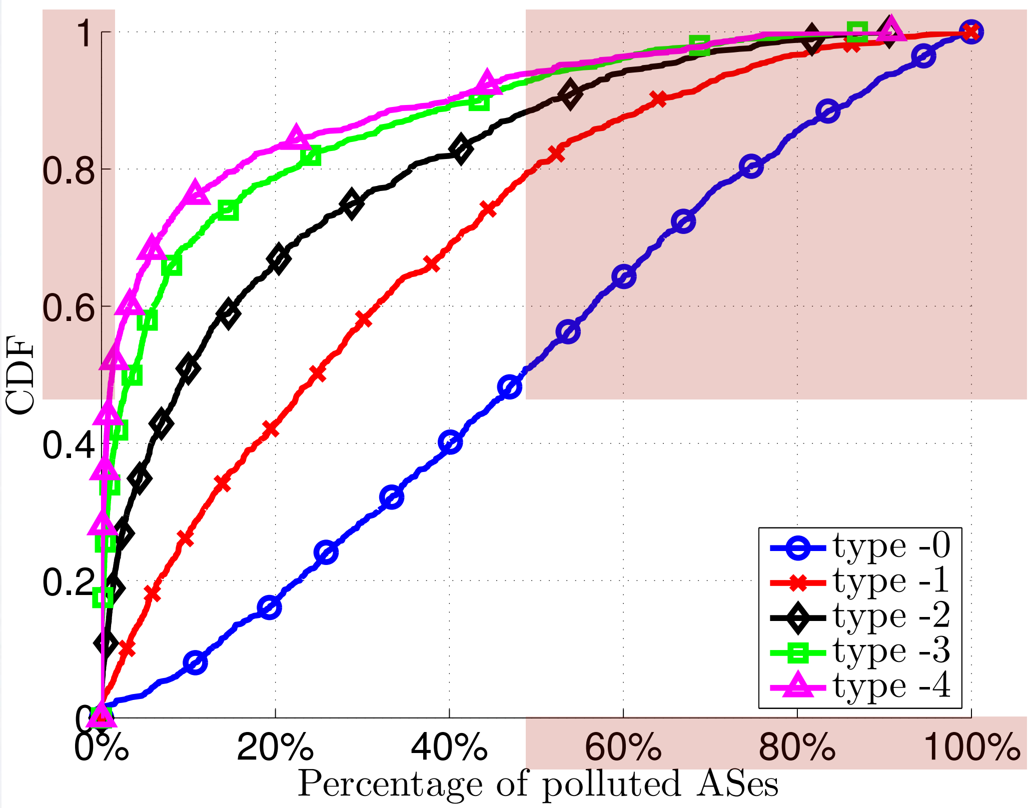
causing: service disruption, fraud, data theft, bad reputation, …

ATTACKS UNDER THE RADAR

can have large impact

- Hijack Types:
  - **Type 0** hijack: <*prefix:* ***BAD_AS****, …*>   *(a.k.a. "prefix origin hijack")*
  - **Type 1** hijack: <*prefix: oAS,* ***BAD_AS****, …*>
  - **Type 2** hijack: <*prefix: oAS, AS1,* ***BAD_AS****, …*>
  - …

lots of attention



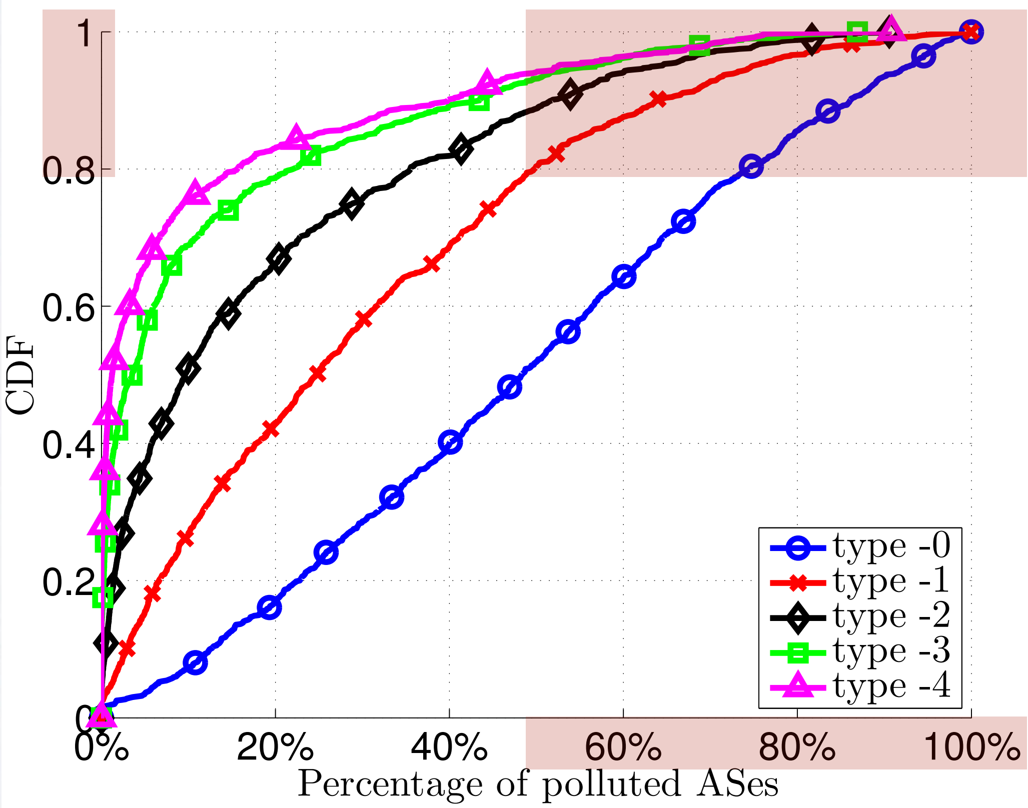
Center for Applied Internet Data Analysis
University of California San Diego

Foundation for Research and Technology-Hellas
University of Crete,

ATTACKS UNDER THE RADAR

can have large impact

- Hijack Types:
  - **Type 0** hijack: <*prefix:* ***BAD_AS***, …>   (*a.k.a. "prefix origin hijack"*)
  - **Type 1** hijack: <*prefix: oAS,* ***BAD_AS***, …>
  - **Type 2** hijack: <*prefix: oAS, AS1,* ***BAD_AS***, …>
  - …



often neglected

Center for Applied Internet Data Analysis
University of California San Diego

Foundation for Research and Technology-Hellas
University of Crete,

STATE OF THE ART

False Positives + False Negatives

- **Third-party Detection Services**
  - False Positives
    - unless you promptly communicate changes to your network configuration
    - Privacy?
  - False Negatives
    - Most services focus on *Type-0* attacks
    - Hard to detect more sophisticated attacks *(Type-1, Type-2, …)*
  - Mitigation?
    - No integration with mitigation solutions
    - *Btw, would you mitigate if uncertain? how later?*

NEED

EARLY & ACCURATE DETECTION

+

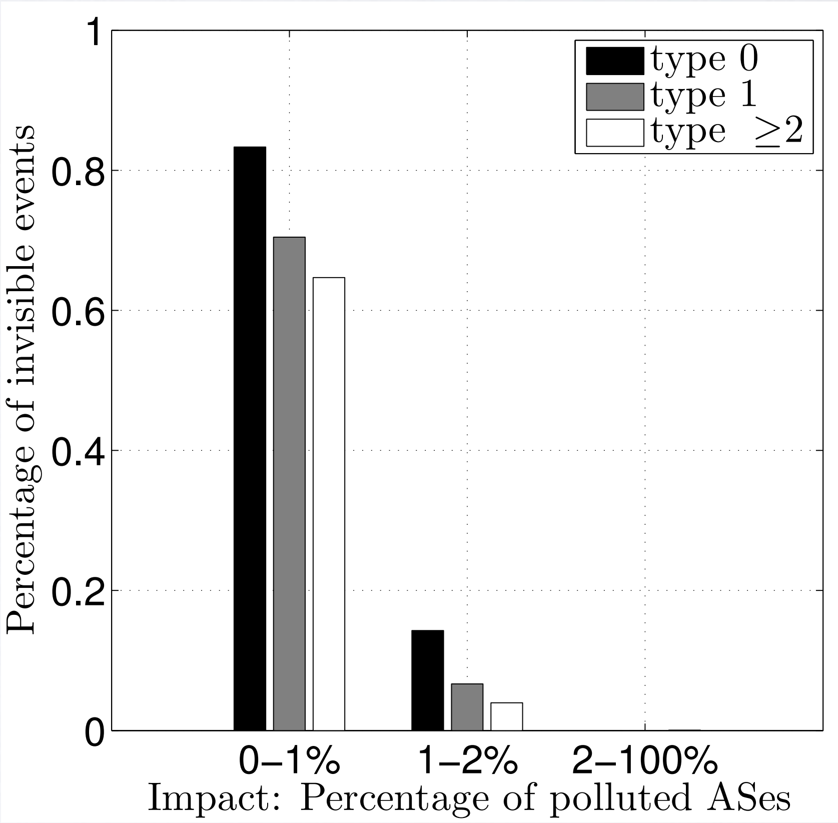
FAST MITIGATION

OUR APPROACH

ARTEMIS (1/3)

- **Realtime BGP Monitoring** using public infrastructure
  - ~200 vantage points worldwide (BGP routers)
    - source: *RouteViews, RIPE RIS, Colorado State Univ. BGPMon*
    - processing: CAIDA's *BGPStream*

- **Provides visibility of all impactful events**



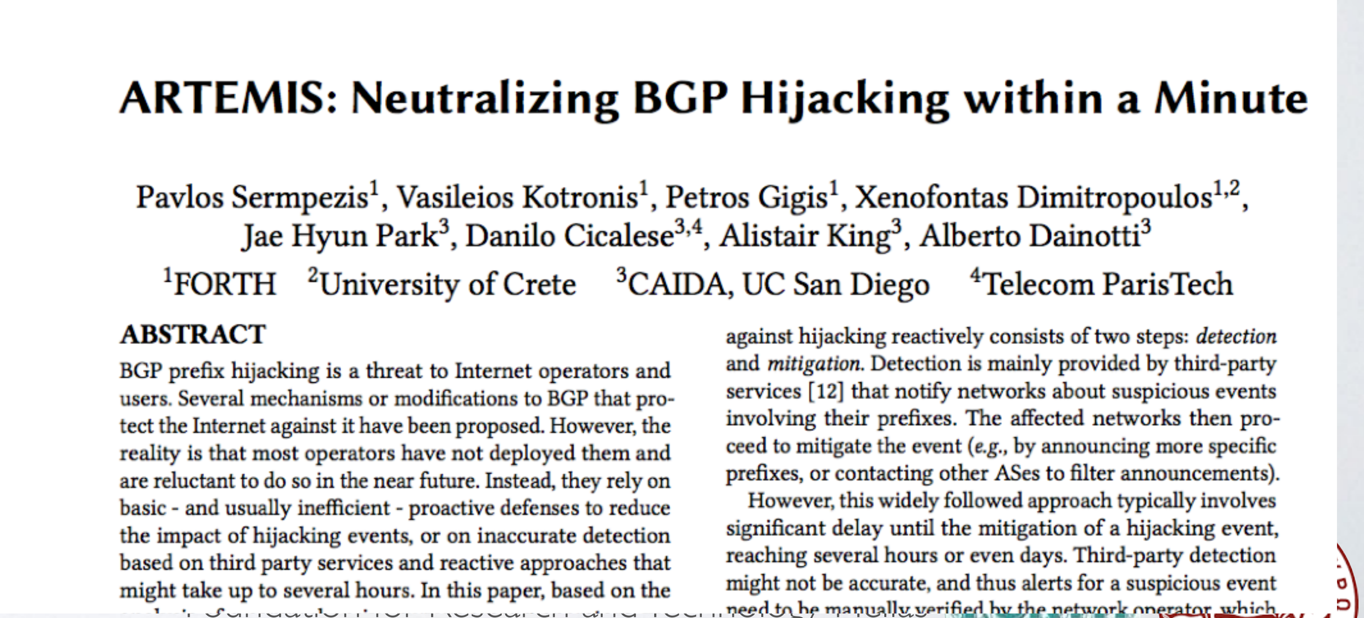
- **Detect events in few seconds!**

(tested with experiments on the real Internet)

OUR APPROACH

ARTEMIS (2/3)

- **Detection without outsourcing**
  - Run locally: leverages knowledge of your network configuration
  - Accurate:
    - Detects *all* types of attacks!
    - No *false negatives* for all visible attacks
    - No *false positives* for most types of attacks;
      - demonstrated extremely low rate otherwise
  - No sharing of private data
  - Transparency: open source code



ARTEMIS: Neutralizing BGP Hijacking within a Minute

Pavlos Sermpezis[1], Vasileios Kotronis[1], Petros Gigis[1], Xenofontas Dimitropoulos[1,2],
Jae Hyun Park[3], Danilo Cicalese[3,4], Alistair King[3], Alberto Dainotti[3]

[1]FORTH [2]University of Crete [3]CAIDA, UC San Diego [4]Telecom ParisTech

ABSTRACT

BGP prefix hijacking is a threat to Internet operators and users. Several mechanisms or modifications to BGP that protect the Internet against it have been proposed. However, the reality is that most operators have not deployed them and are reluctant to do so in the near future. Instead, they rely on basic - and usually inefficient - proactive defenses to reduce the impact of hijacking events, or on inaccurate detection based on third party services and reactive approaches that might take up to several hours. In this paper, based on the

against hijacking reactively consists of two steps: *detection* and *mitigation*. Detection is mainly provided by third-party services [12] that notify networks about suspicious events involving their prefixes. The affected networks then proceed to mitigate the event (*e.g.*, by announcing more specific prefixes, or contacting other ASes to filter announcements).

However, this widely followed approach typically involves significant delay until the mitigation of a hijacking event, reaching several hours or even days. Third-party detection might not be accurate, and thus alerts for a suspicious event need to be manually verified by the network operator, which

OUR APPROACH

ARTEMIS (3/3)

- **Mitigation**
  - Automated + flexible (it can be configured on a per-prefix basis)
  - Both autonomous or outsourced
    - Prefix de-aggregation
    - Announcement and tunneling from other ASes
    - Contact offending AS and its neighbors

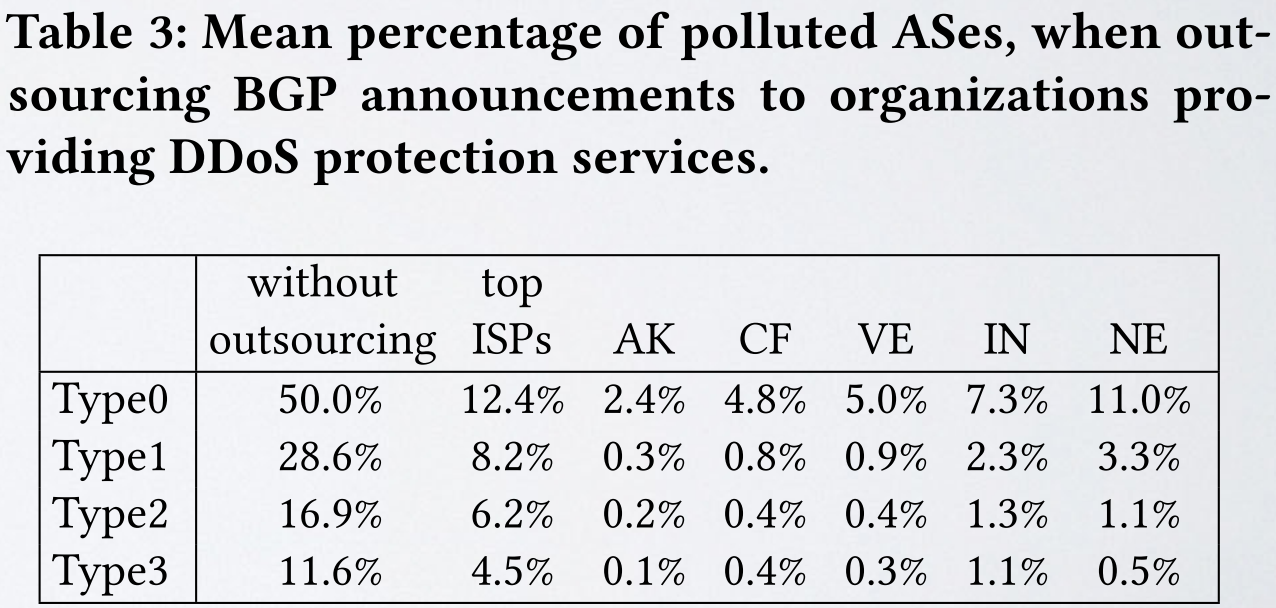


Table 3: Mean percentage of polluted ASes, when outsourcing BGP announcements to organizations providing DDoS protection services.

	without outsourcing	top ISPs	AK	CF	VE	IN	NE
Type0	50.0%	12.4%	2.4%	4.8%	5.0%	7.3%	11.0%
Type1	28.6%	8.2%	0.3%	0.8%	0.9%	2.3%	3.3%
Type2	16.9%	6.2%	0.2%	0.4%	0.4%	1.3%	1.1%
Type3	11.6%	4.5%	0.1%	0.4%	0.3%	1.1%	0.5%

ARTEMIS CONFIGURATION

sample

- **Configuration file**
  - configure manually
  - extract from routers / route reflector
  - pre-populate from RADB?
  - …

```
// Artemis configuration for our main prefixes
prefixes: 123.123.0.0/16, 111.111.111.0/24
   origin_asns: 4131, 4132
   neighbors: 4000, 3112, 2670, 45, 2800, 7462, 4123
   mitigation: deaggregate

// Artemis configuration for prefixes we use only at site #2
prefixes: 123.124.125.0/24, 222.222.222.0/24
   origin_asns: 4131
   neighbors: 2800, 7462, 4123
   mitigation: deaggregate, outsource
```

PILOT DEPLOYMENT

try ARTEMIS

- **Pilot** deployment of detection component
  - *all you need is a box with Python*
- Feedback
- Read our paper draft
- Contribute to the development of scripts etc.

THANKS

alberto@caida.org

ONE LAST SLIDE

*- We are also developing a centralized service (**an Internet observatory for BGP hijacks and anomalies**) which does not need deployment in your network*

- Soon you'll be able to subscribe to receive notifications and inspect events on a dashboard

- If you upload your ARTEMIS configuration file it is going to be more accurate and may provide more information about the incident